CLAIMS

1. A method for transporting encrypted media, comprising:

receiving a request to transport encrypted Internet Protocol (IP) media packets over a circuit switched network;

establishing an IP link over the circuit switched network; and

transporting the encrypted IP media packets over the IP link established over the circuit switched network.

2. A method according to claim 1 including establishing a data channel over the circuit switched network and using a Point to Point Protocol over the data channel to establish the IP link.

3. The method according to claim 2 including establishing the data channel over an Integrated Services Digital Network (ISDN) channel of a Public Services Telephone Network.

4. A method according to claim 1 including transporting the encrypted IP media packets over the packet switched network without decrypting or decoding the media in the encrypted IP media packets.

5. A method according to claim 1 including:

receiving call requests from endpoints connected to the packet switched network;

identifying the call requests that require IP encryption;

identifying ingress devices in the circuit switched network associated with the identified call requests that support transport of the encrypted IP media packets over the circuit switched network;

establishing IP links over the circuit switched network with the identified egress devices; and

transporting the encrypted IP media packets to the identified ingress devices.

6. A method according to claim 5 including:

identifying non-supporting ingress devices in the circuit switched network associated with the identified call requests that do not support transport of encrypted IP media packets over the circuit switched network;

establishing circuit switched connections over the circuit switched network for the identified non-supporting egress devices;

decrypting and decoding media in the encrypted IP media packets associated with the non-supporting egress devices; and

re-encoding and re-encrypting the media into a circuit switched network format; and

transporting the re-encoded and re-encrypted media over the circuit switched connections to the non-supporting egress devices.

7. A method according to claim 1 including:

authenticating an ingress device associated with the IP media packets;

sending a first encrypted key associated with a first endpoint over the circuit switched network to the authenticated ingress device;

receiving a second encrypted key over the circuit switched network from the authenticated ingress device associated with a second endpoint;

decrypting the second key and forwarding the decrypted second key over the packet switched network to the first endpoint;

encrypting media at the first endpoint directed to the second endpoint using the first key; and

decrypting encrypted IP media packets at the first endpoint received from the second endpoint using the second key.

8. A method according to claim 1 including encrypting the IP media packets only once at a first sending endpoint and decrypting the IP media packets only once at a receiving second endpoint.

9. A method according to claim 1 including:

encrypting the IP media packets using a Secure Real-time Transport Protocol (SRTP);

establishing a Point to Point Protocol (PPP) connection over an Integrated Services Digital Network (ISDN) channel in the circuit switched network; and

sending the SRTP encrypted IP media packets over the PPP connection.

10. A network processing device, comprising:

a processor configured to establish a connection between two endpoints that extends over an Internet Protocol (IP) network and a circuit switched network, the processor forwarding packets having an encrypted IP packet payload between the two endpoints without decrypting the encrypted IP packet payload when transferred between the IP network and circuit switched network.

11. A network processing device according to claim 10 wherein the processor establishes an IP link over the circuit switched network and forwards the encrypted IP packet payload over the IP link.

12. A network processing device according to claim 10 wherein the processor selects a first codec when the encrypted IP packet payload is decrypted for transport over a PSTN connection in the circuit switched network and selects a second codec with higher compression when the encrypted IP packet payload is not decrypted and transported over a data link in the circuit switched network.

13. A network processing device according to claim 10 including a memory containing a dial plan for identifying phone numbers that can be transferred between the IP network and the circuit switched network without decrypting the encrypted IP packet payload.

14. A network processing device according to claim 10 including memory for storing a shared key shared with an ingress device located at an ingress side of the IP network, the processor receiving a first key from a first endpoint, encrypting the first key using the shared key and sending the encrypted first key to the ingress device.

15. A network processing device according to claim 14 wherein the processor receives a second encrypted key from the ingress device, the processor decrypting the

encrypted key using the shared key and then forwarding the second decrypted key to the first endpoint.

16. A network processing device according to claim 10 wherein the processor conducts a Point to Point Protocol over an Integrated Services Digital Network (ISDN) channel for establishing an IP link over the circuit switched network and then forwards Secure Real-time Transport Protocol (SRTP) encrypted IP packet payloads over the IP link.

17. A method for transporting encrypted media, comprising:

receiving call requests from endpoints;

identifying call requests requiring media encryption;

directing endpoints for the identified call requests to encrypt media using an Internet Protocol (IP) encryption protocol;

identifying the call requests that also require connections over a Public Services Telephone Network (PSTN);

establishing data links over the PSTN for the identified call requests;

receiving IP encrypted media from the endpoints for the identified call requests; and

forwarding the IP encrypted media over the data links established on the PSTN.

18. The method according to claim 17 including:

authenticating the identified call requests with ingress gateways;

conducting Point-to-Point Protocol (PPP) sessions with the ingress gateways when the ingress gateways are authenticated; and

exchanging encryption keys with the ingress gateways during the PPP session.

19. The method according to claim 18 including:

encrypting the encryption keys using keys shared with the ingress gateways; and

sending the encrypted encryption key to the ingress gateways.